IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM

DECLARATION OF LEE ZIMMERMAN IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Lee Zimmerman, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

I. INTRODUCTION

1. I have been employed by SolarWinds (the "Company") since 2010 and currently hold the position of Senior Manager. Throughout my employment at SolarWinds, I have been responsible for release management—the process by which SolarWinds software is made available to customers. I make this declaration in support of SolarWinds' and Tim Brown's motion for summary judgment. The facts set forth herein are based on my personal knowledge and my review of SolarWinds records. If called upon to do so, I can and will competently testify to these facts.

2. I understand the Securities and Exchange Commission (SEC) relies on certain emails, including emails I am on, concerning a report from a security researcher (the "Security Researcher") about a password for an account on a third-party server used by SolarWinds, which the Security Researcher found in a publicly searchable code repository. I write to clarify certain facts about this incident, which I investigated in response to the Security Researcher's report.

3. The password at issue—"solarwinds123"—was for an account (the "Account") on a File Transfer Protocol or "FTP" server hosted by Akamai, a third-party service provider (the "Akamai Server"). *See* Ex. A (SW-SEC00001476) at -483-84. An FTP server is designed to facilitate the upload or download of large files. I am fully familiar with the Akamai Server, as it was used as part of our infrastructure for distributing software to customers.

4. Specifically, at the time of the Security Researcher's report, SolarWinds software files would be distributed to customers by uploading the files to the Akamai Server, and then publishing links to the files on SolarWinds' customer websites—solarwinds.com and customerportal.solarwinds.com ("the SW Websites"). By clicking on the links, customers could download the files from the Akamai Server. The Account was a seldom-used backup account on the Akamai Server, which had the ability to upload files to the Akamai Server.

5. As I know from my investigation of the Security Researcher's report, the password for the Account had been used for a coding project by a SolarWinds intern, who in March 2018 uploaded the code for that project to a cloud-based code repository that, unknown to SolarWinds at the time, the intern accidentally made publicly searchable. The Security Researcher later discovered the password in the repository and reported the issue to SolarWinds on November 19, 2019. Ex. A at -484.

6. I understand the SEC has alleged that the "solarwinds123" password for the Account contradicts the statement in SolarWinds' online Security Statement that the Company's "best practices enforce the use of complex passwords." However, it is only possible to enforce password complexity automatically on systems that provide that functionality. SolarWinds did not have the ability to automatically enforce its password requirements on the Akamai Server. The server did not reside on SolarWinds' network. It was maintained by a third party—Akamai. And

the server did not have any functionality that enabled SolarWinds to automatically enforce its password complexity requirements on user accounts.

7. I further understand that the SEC has alleged that, if the password for the Account had been discovered by a malicious actor, it could have been used to distribute malicious files to SolarWinds customers. That scenario was highly unlikely for two reasons.

8. First, while the Account had the ability to upload files to the Akamai Server, doing so would *not* make links to the files available on the SW Websites. Publishing links on the SW Websites required access to the servers hosting the SW Websites, which the Account did not have. Nor could the Account be used to replace files on the Akamai Server that were already linked to on the SW Websites, by uploading files with the same filenames as those existing files. Files uploaded to the Akamai server would only be uploaded to a staging area. They would not replace existing files without separate action being taken to purge those existing files—which the Account did not have the necessary permissions to do. So, even if a malicious actor gained access to the Account, that would not have given the actor the ability to alter the software available for download on the SW Websites.

9. Second, like most software companies, SolarWinds digitally signs its software before publishing it. It is common in the industry for software customers to check that a vendor's software is digitally signed before installing it. So, even if a malicious actor did find a way to trick SolarWinds customers into downloading files that the actor uploaded to the Akamai Server, the files would be unsigned by SolarWinds and customers could easily detect that they were inauthentic.

10. Finally, I want to note that SolarWinds promptly remediated the leak of the password for the Account as soon as it was discovered. After receiving the Security Researcher's

Report on November 19, 2019, I immediately changed the password for the Account. As a precaution, I also checked the files on the Akamai Server and confirmed that none of them had been tampered with (as reflected by the fact that they were all digitally signed by SolarWinds). Our investigation found no indication that the Account was ever used by any unauthorized actor.

[*signature on following page*]

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 23, 2025

Lee Zimmerman